Provisional Translation (as of November 2023)[*]

PSEHB/MDED Notification No.0523-1
May 23, 2023

To: Directors of Prefectural Health Departments (Bureaus)

Director of the Medical Device Evaluation Division,
Pharmaceutical Safety and Environmental Health Bureau,
Ministry of Health, Labour and Welfare
(Official seal omitted)

Confirmation of compliance with Article 12, Paragraph 3 of the Essential Principles for Medical Devices

Article 12, Paragraph 3, which is stipulated in the revised "Standards for Medical Devices Prescribed by the Minister of Health, Labour and Welfare pursuant to the provisions of Article 41, Paragraph 3 of the Act on Securing Quality, Efficacy and Safety of Products including Pharmaceuticals and Medical Devices (Ministerial Notification No. 122 of 2005; hereinafter referred to as the "Essential Principles")" by Ministerial Notification No. 67 of 2023 has been established a transitional measure period of one year and that for medical devices requiring compliance with the Article 12, Paragraph 3 of the revised Essential Principles, the provisions then in force shall remain applicable until April 1, 2024.

Confirmation of conformity shall be made as follows. Please inform thoroughly the relevant organizations and the related marketing authorization holders under your supervision.

Please note that copies of this notification will be sent to the President of the Pharmaceuticals and Medical Devices Agency, the President of the Japan Federation of Medical Devices Associations, the President of the American Medical Devices and Diagnostics Manufacturers' Association, the Chairman of the Medical Equipment Committee of European Business Council in Japan, the Chairman of the IVD Committee of European Business Council in Japan, the Chairman of the Japan Association of Clinical Reagents Industries and the President of the Association of Registered Certification Bodies under PAL.

***

[*] This English version of the Japanese Notification is provided for reference purposes only. In the event of any inconsistency between the Japanese original and the English translation, the former shall prevail.

In order to demonstrate compliance with Article 12, Paragraph 3 of the Essential Principles for Medical Devices, the marketing authorization holder, etc., who applies for approval or certification of specially-controlled medical devices or controlled medical devices, shall confirm conformance to JIS T 81001-5-1, etc. with regard to the following matters and specify the internal documents, etc. that show the results or summarize the results. It is necessary to confirm conformance of general medical devices in the same way.

1. Requirements relating to JIS

(1) General Requirements in Clause 4 of JIS T 81001-5-1

- Implement activities to ensure cybersecurity on the basis of quality management system.
- Establish activities to notify the vulnerabilities for regulatory authorities and customers.
- Risk management of medical devices shall consider the security vulnerabilities and threats, etc.

(2) Software Development Process in Clause 5 of JIS T 81001-5-1

According to JIS T 81001-5-1, the software development process shall have the following considerations.

- Consider the security updates handling and development environment security in development planning.
- Identify security requirements, including product security capabilities.
- Implement the architectural design considering the intended environment of use, trust boundary and defense-in-depth etc.
- Design and implement considering the secure design best practices.
- Perform software system testing to ensure that security requirements are met and that the methods to address threats identified in the risk management process are implemented in the design and are effective.

(3) Software Maintenance Process in Clause 6 of JIS T 81001-5-1

Establish a policy for notifying customers about security updates.

(4) Risk Management Process related to the Security in Clause 7 of JIS T 81001-5-1

In the risk management of medical devices, identify the relevant vulnerabilities, estimate and assess the relevant threats, control the threats with risk control measures, and monitor their effectiveness, taking into account the intended use and intended environment of use of the medical device.

(5) Software Configuration Management Process in Clause 8 of JIS T 81001-5-1

Establish a configuration management process with change control and change history for

the development, maintenance and support of the medical device.

(6) Software Problem Resolution Process in Clause 9 of JIS T 81001-5-1

Establish the procedures for communicating and handling information about security vulnerabilities and handle security issues including information disclosure in accordance with the procedures.

2. Requirements for existing notifications etc. related to JIS

The following items shall be additionally confirmed when confirming conformity to the standard.

(1) General Requirements in Clause 4 of JIS T 81001-5-1

As required in the “Guidance on Ensuring Cybersecurity of Medical Devices” (PSEHB/MDED Notification No. 0724-1 and PSEHB/PSD Notification No. 0724-1 dated July 24, 2018), the security policy and customer contact points for security shall be clarified in the quality management system and it shall be confirmed by establishing procedures for disclosing vulnerabilities to customers.

(2) Software Development Process in Clause 5 of JIS T 81001-5-1

As specified in Article 12, Paragraph 3 of the Essential Principles, it is necessary to identify the security requirements based on the operating environment and network use environment, etc. of the medical device. It shall be confirmed using, for example, the system configuration diagram or network configuration diagram for the intended environment of use.

(3) Software Maintenance Process in Clause 6 of JIS T 8101-5-1

As a “plan to ensure cybersecurity throughout the total life cycle of the medical devices” stipulated in Article 12, Paragraph 3 of the Essential Principles, the software maintenance plan shall establish a plan for the product life cycle such as end of support, and a plan for implementing future measures to address vulnerabilities such as vulnerability monitoring and security updates. As part of the plan, the policy for notifying customers of security updates shall be clarified.

(4) Software Configuration Management Process in Clause 8 of JIS T 81001-5-1

Configuration management processes shall be confirmed by preparing the software bill of materials (SBOM) of the medical device appropriately.

Reference: Compliance with the Essential Principles Check List

Essential Principles	Applied/ Not applied	Method for Compliance	Identity of Specific Documents
(Consideration of medical devices using software)			
3 For medical devices using software that are used in connection with other devices and networks, etc., or that may be subject to external unauthorized access and attack, etc., appropriate requirements shall be identified, taking into account the operating environment and network use environment of the medical device, the risk related to cybersecurity that may affect the function of the medical device or cause safety concerns shall be identified and evaluated, and risk management shall be conducted to reduce such cyber risks. In addition, such medical devices shall be designed and manufactured based on a plan to ensure cybersecurity throughout the total product life cycle of the medical device.	Applied	Demonstration of compliance with the applicable items of the recognized criteria.	"Confirmation of compliance with Article 12, Paragraph 3 of the Essential Principles for Medical Devices" (PSEHB/MDED Notification No.0523-1, May 23, 2023)